REMARKS

Claims 1, 3-6, 8, 11, 13, 15-19, 22-25, 27, 28, 34, 35 are amended. Support for the amendments of claims 1, 3, 5, 6, 8, 11, 13, 15, 16, 18, 19, 22, 23, 24, 25, 27, 28, 34, and 35 can be found in the original claims and page 16, line 9 to page 18, line 6, and page 12, line 21 to page 13, line 6 of the present Application. No new matter has been added.

Claims 1-11, 21, 25, and 29 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. In response, Applicants amended claims 1, 3-6, 8, 11, and 25 to define a computer-readable recording, and cancelled claims 2, 7, 9-10, and 29. For this reason, withdrawal of the §101 rejection is respectfully requested.

Claims 1-24, 29-34, and 36-40 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel et al. (U.S. Patent No. 7,159,149), in view of Willebeek-LeMair et al. (U.S. Publication No. 2003/0204632). Applicants respectfully traverse the rejections of these claims based upon the amendments to the claims.

Independent claims 1, 13, and 15, as amended, recite "changing the setting information upon it being judged at the judging that the communication is executed by the worm". Claims 2 and 14 have been cancelled.

The Examiner asserts that Spiegel discloses the above feature of the present invention at col. 5, lines 15-21 and col.6, lines 15-22.

However, Spiegel's technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system. Spiegel fails to disclose or suggest "changing the setting information upon it being judged at the judging that the communication is executed by the worm". Willebeek-LeMair also fails to disclose or suggest this feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the above feature of the present invention. Therefore, amended claims 1, 13, and 15 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

Claims 4 and 17, as amended, depend from claims 1 and 15, and claims 4 and 17 include all of the features of independent claims 1 and 15 plus additional features which are not disclosed or suggested by the cited references, respectively. Therefore, claims 4 and 17 are also submitted to be patentable over the cited references.

Independent claims 3 and 16, as amended, recite "changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm". The Examiner asserts that Spiegel discloses this feature of the present invention at col. 5, lines 15-21 and col.6, lines 15-22.

However, Spiegel's technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system. Spiegel fails to disclose or suggest "changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm". Willebeek-LeMair also fails to disclose or suggest the feature of the present invention. Thus, even if one were to combine the disclosure of these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claims 3 and 16 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

New claim 41 depends from claim 3 and includes all of the features of independent claim 3 plus additional features which are not disclosed or suggested by the cited references, respectively. Therefore, new claim 41 is also submitted to be patentable over the cited references.

Independent claims 5 and 18, as amended, recite "judging that a communication from a plurality of computers in the predetermined segment is executed by the worm when a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside".

The Examiner asserts that Spiegel discloses the above feature of the present invention at col. 5, lines 8-10, col. 5, lines 47-50, and col. 3, lines 20-27.

However, Spiegel merely discloses that the threshold criteria are based on historical data for failed connection attempts (col. 5, lines 8-10). The failed attempts are weighted according to an attribute thereof, such as the source of the failed attempt or the destination address (see col. 5, lines 47-50 of Spiegel), and if infected, a process is likely to produce a relatively large number of connection attempts to remote destination addresses over a given period of time (see col. 3, lines 20-27 of Spiegel).

Spiegel fails to disclose or suggest "judging that a communication from a plurality of computers in the predetermined segment is executed by the worm when a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside, and the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside" (Emphasis added). Willebeek-LeMair also fails to disclose or suggest the above feature of the present invention. Thus, even if one were to combine the disclosure of these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claims 5 and 18 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

Independent claims 6 and 19, as amended, recite "judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and there is an increase in number of sender addresses of the responding communication packets".

The Examiner asserts Spiegel discloses that the above feature of the present invention at col. 4, lines 17-22.

However, Spiegel merely discloses that a source is more likely to be infected if the number of unique addresses of its failed connection attempts is high.

Spiegel fails to disclose or suggest "judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and there is an increase in number of sender addresses of the responding communication packets" (Emphasis added). Willebeek-LeMair also fails to disclose or suggest the feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claims 6 and 19 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

New claim 42 depends from claim 6, and includes all of the features of independent claim 6 plus additional features which are not disclosed or suggested by the cited references, respectively. Therefore, new claim 42 is also submitted to be patentable over cited references.

Independent claim 8, as amended, recites "predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance". The Examiner asserts that Spiegel discloses that the above feature of the present invention at col. 3, lines 58-67 and col. 5, lines 8-15.

However, Spiegel merely discloses that the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. Spiegel fails to disclose or suggest "predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance" (Emphasis added). Willebeek-LeMair also fails to disclose or suggest the feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claim 8 is submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

New claim 43 depends from claim 8, and includes all of the features of independent claim 8 plus additional features which are not disclosed or suggested by the cited references, respectively. Therefore, new claim 43 is also submitted to be patentable over cited references.

Independent claim 11, as amended, recites "cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have a worm". The Examiner asserts that Spiegel discloses that the above feature of the present invention at col. 6, lines 48-55.

However, Spiegel merely discloses that other methods of observing the connection attempts include implementing a network card shim, hooking the TDI layer, using MICROSOFT Firewall APIs. Spiegel fails to disclose or suggest "cutting off the communication executed by the worm by making a fire wall function effective" (Emphasis added). Willebeek-LeMair also fails to disclose or suggest the feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claim 11 is submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair.

Independent claims 22, 23, 24, 34, as amended, recite "summing [sums] up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging [by the worm judging unit], and extracting [extracts] as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging". Claim 21 has been cancelled. The Examiner asserts that Willebeek-LeMair discloses that the above feature of the present invention in Willebeek-LeMair paragraph [0031], lines 5-14.

However, Willebeek-LeMair merely discloses that the extraction of packet features may comprise features from the header portion (such as, for example, destination and source IP address, destination and source ports, and the like). Spiegel fails to disclose or suggest "summing [sums] up a number of the communication packets for each port number, the communication packets being transmitted in the communication upon it being judged that the communication is executed by the worm at the judging [by the worm judging unit], and extracting [extracts] as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging" (Emphasis added). Spiegel also fails to disclose or suggest the feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the feature of the present invention. Therefore, amended claims 22, 23, 24, 34 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel and Willebeek-LeMair. For all these reasons, withdrawal of the §103(a) rejection is respectfully requested.

Claims 25, 26, 27, 28, and 35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel and Willebeek-LeMair, in view of Bunker et al. (U.S. Publication No. 2003/0056116). Applicants respectfully traverse the rejections of these claims based on the amendments to these claims.

Independent claims 25, 27, 28, 35, as amended, recite "summing [sums] up, for each direction of communication of a packet transmitted out from the predetermined network segment or to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting [extracts], as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value" (Emphasis added). Claim 26 has been cancelled. The Examiner asserts that Bunker discloses that the above feature of the present invention in paragraph [0189], lines 1-11, paragraph [0215], lines 1-5, paragraph [0220], lines 8-12.

However, Bunker merely discloses that the format of an Enterprise-Wide Summary report includes: number of host tested; number of new hosts appearing on network; total number of vulnerabilities discovered; number of vulnerabilities discovered, by risk level; etc. Bunker fails to disclose or suggest "summing [sums] up, for each direction of communication of a packet transmitted out from the predetermined network segment or to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging" (Emphasis added). Spiegel and Willebeek-LeMair also fail to disclose or suggest the above feature of the present invention. Thus, even if one were to combine these cited references, the resulting combination would not disclose the above feature of the present invention. Therefore, amended claims 25, 27, 28, 35 are submitted to be patentable under 35 U.S.C. §103(a) over Spiegel, Willebeek-LeMair and Bunker.

For all of the foregoing reasons, Applicants submit that this Application is in condition for allowance, which is respectfully requested. The Examiner is invited to contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By Joseph P. Fox
Joseph P. Fox
Registration No. 41,760

July 10, 2008
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
(312) 360-0080
Customer No. 24978